REMARKS

This amendment is filed in response to the Office Action dated October 24, 2008. In that Action, the Examiner rejected Claim 10 under 35 U.S.C. §103(a) as being unpatentable over Arnold in view of Aoki, Epstein, Rose and Shaw. Claim 11 was rejected under §103(a) as being unpatentable over Arnold in view of Aoki, Epstein, Rose, Shaw and Sandhu. Claims 12 and 25-26 were rejected under §103(a) as being unpatentable over Arnold in view of Aoki, Epstein, Rose, Shaw, Sandhu and Davis.

With regard to the rejection of independent Claims 10 and 25, Applicants would respectfully submit that the proposed combinations do not render the present invention obvious because the references fail to disclose or suggest, either alone or in combination, the generation or reception of a server message having application code in first and second portions wherein the first portion is small relative to the second portion, and the first portion is public key encrypted while the second portion is not public key encrypted so the first portion is authenticated using a server public key while the second portion can be authenticated using a less computationally expensive algorithm. The Office Action acknowledges that none of Arnold, Aoki or Epstein teach the generation of a message including application code having first encrypted portion separate from a second portion, and relies on Rose for this feature. However, Rose still encrypts the entire message using a public key algorithm. The relevant text of Rose is found at column 5, lines 44-49 which states that the control information (reference numeral 182) is first encrypted with the server's private key, and then the entire file (which includes all of the application code) is encrypted with the user's public key. Rose accordingly does not achieve the efficiencies of the present invention by using a less computationally expensive authentication on the greater portion of the application code, but instead results in more required computations since there is "double" encryption. Indeed, Rose states at column 5, lines 49-52 that none of the application program should appear as plain text, i.e., all of it should be public key encrypted, which teaches against Applicants' invention.

Moreover, the element of Rose which the Office Action identifies as corresponding to Applicants' claimed "first portion" of application code is not actually application code. That element is the control information 182, which may be broken down into header fields 183, 184

and 185. Those fields represent an application identification number (ID), a licensee ID, and a license termination date. Element 182 thus does not contain any application code, which is further made clear by the presence of separate element 181 (the "Application Program"). Rose never breaks up the Application Program 181 into two portions having different authentications. This interpretation of Rose is thus clearly erroneous, and one skilled in the art would not be motivated by the teachings of Rose to even try splitting up the application code.

The Office Action also acknowledges that none of Arnold, Aoki, Epstein or Rose teaches the first portion of application code being small relative to the second portion, or that the second portion is authenticated using a non-public key algorithm, and relies on Shaw for this feature. However, Shaw does not use separate authentication algorithms for different portions of the downloaded application code. Shaw states at column 3, lines 33-44 that, as part of the boot process when the computer system is first turned on (or after system reset), the boot code performs an integrity check on application code, but this application code already resides on the computer system. It is not part of any message from a server to the client. The integrity check is performed on the entire application code, and not just a portion of it. Downloading is performed only after it is determined that the application code is corrupt; see column 4, lines 3-5. The MD5 verification is hashed based, and Shaw refers to it as a digest technique. When the application code is updated via download, the same hash or digest algorithm is used to validate each segment of the application code; see column 4, lines 46-49. Validation of the updater code is also performed using a "digest"; see column 4, lines 23-26.

Shaw further lacks any indication that one portion of the application code would be smaller than any other portion. In fact, Shaw states that the segments each have the same default size to correspond with a sector of flash memory; see column 5, lines 27-30. Accordingly, the proposed combination including Shaw still fails to result in the use of a more expensive (and more secure) encryption technique for a small portion of application code followed by a less expensive integrity check for a larger portion of the application code.

Each of Applicants' independent claims (Claims 10 and 25) recite the server message including application code having a first portion authenticable with a server public key and a second portion authenticable with an integrity checking algorithm that is not a public key

algorithm. Since the proposed combinations still do not result in the invention as explicitly set forth in Applicants' claims, they accordingly cannot render the present invention obvious. The foregoing arguments apply equally to the remaining §103(a) rejections of the dependent claims inasmuch as those rejections are based on the combination of Arnold, Aoki, Epstein, Rose and Shaw.

Notwithstanding the foregoing, Applicants have amended Claims 10 and 25 to clarify that the second portion of the application code is not encrypted by a public key algorithm, and that the second portion is authenticated by an integrity checking algorithm that is less computationally expensive than a public key algorithm. These amendments serve to further distinguish Applicants' invention from the cited references. For all of the foregoing reasons, Applicants respectfully request reconsideration of the §103(a) rejections.

Applicants have made a diligent effort to advance the prosecution of this application by amending claims and pointing out with particularity how the claims as presented patentably define the invention over the prior art of record. In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned.

Respectfully submitted,

/Jack V. Musgrove/

Jack V. Musgrove
Attorney for Applicant(s)
Reg. No. 31,986
Telephone: 512-689-6116